IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NORTH CAROLINA

SYLVIA TOMPKINS, KENNETH BRENNAN, and CHANDRA BROWN on behalf of themselves and all others similarly situated, Plaintiffs, v. US RADIOLOGY SPECIALISTS, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Sylvia Tompkins, Kenneth Brennan, and Chandra Brown, individually and on behalf of all others similarly situated ("Class Members"), bring this Class Action Complaint against US Radiology Specialists, Inc., ("US Radiology" or "Defendant"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard sensitive information entrusted to it, including, without limitation, Plaintiffs' and Class Members': names, addresses, dates of birth, social security numbers, health insurance information, medical record numbers, patient account numbers, physician information, dates of medical services, and diagnosis and treatment information related to radiology services.

2. US Radiology partners with radiology providers nationwide to provide "elevated patient care" across the country. US Radiology claims it has the tools and resources radiology providers require to help the business side of their practices flourish, enabling the radiology

provider partners to focus on patient care.[1]

3. US Radiology has at least ten radiology provider partners who provide patient care to individuals in New York, New Jersey, North Carolina, South Carolina, Georgia, Florida, Alabama, Arkansas, Texas, Oklahoma, Kansas, Colorado, Nebraska, Arizona, and Montana. According to US Radiology's website, its partners include Charlotte Radiology, Diversified Radiology, Touchstone Medical Imaging, American Health Imaging, Radiology Ltd, Upstate Carolina Radiology, Windsong Radiology, Gateway Diagnostic Imaging, South Jersey Radiology Associates, and Larchmont Imaging Associates (collectively, the "Partners").[2]

4. On various dates throughout 2022, Partners announced that between December 17 and December 24, 2021, an unauthorized, unknown third party gained access to their computer network, resulting in the unauthorized access or acquisition of the personal identifying information[3] ("PII") and protected health information ("PHI") of Plaintiffs and Class Members (the "Data Breach").

5. While each Partner announced the Data Breach individually, their Data Breach Notice Letters are near identical in both form and substance. In what Plaintiffs allege is a complete lack of transparency, the Notice Letters do not mention that the Data Breach is associated with US Radiology and, upon information and belief, occurred through US Radiology.

6. Because the Partners announced the Data Breach individually, the true scope and

[1] *See* https://www.usradiology.com/why-us-radiology (last accessed Oct. 8, 2022).
[2] *See* https://www.usradiology.com/partners (last accessed Oct. 8, 2022).
[3] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

scale of the Data Breach is still unknown. In February 2022, US Radiology notified the U.S. Department of Health and Human Services Office for Civil Rights ("HHS") of a cybersecurity incident that compromised the PII and PHI (collectively, "Personal Information") of 87,552 patients.[4] Thereafter, the Texas Attorney General's Office received reports from both Gateway Diagnostics and American Health Imaging, notifying the Office that the Data Breach impacted 240,673 Texas Gateway Diagnostics patients and 21,003 Texas American Health Imaging patients. Upon information and belief, the total number of Class Members affected by the Data Breach is at least hundreds of thousands.

7. By entering into business relationships with the Partners and through those relationships obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Personal Information, US Radiology assumed legal and equitable duties to protect that Personal Information.

8. The compromised Personal Information of Plaintiffs and Class Members is now, at the very least, in the hands of a hacker who can sell that Personal Information on the dark web to criminals. Plaintiffs and Class Members face a lifetime risk of identity theft resulting from the Data Breach.

9. The Personal Information was compromised due to Defendant's negligent and/or reckless acts and omissions and the failure to protect the Personal Information of Plaintiffs and Class Members.

10. US Radiology failed to timely notify Plaintiffs and Class Members of the Data breach as required by law.

11. Plaintiffs bring this action on behalf of all persons whose Personal Information was

[4] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Sept. 26, 2022).

compromised as a result of Defendant's failure to: (i) adequately protect the Personal Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of its inadequate information security practices; and (iii) avoid sharing the Personal Information of Plaintiffs and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes as alleged below.

12. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of their Personal Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their Personal Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information.

13. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs and Class Members' Personal Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the Personal Information of Plaintiffs and Class Members was compromised through disclosure to and exfiltration by an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that

their information is and remains safe, and they should be entitled to actual, statutory and nominal damages, injunctive and other equitable relief.

II. PARTIES

14. Plaintiff Sylvia Tompkins is a citizen of Texas. Plaintiff Tompkins is a Data Breach victim and a patient of Gateway Diagnostics, a US Radiology Partner. Plaintiff Tompkins was notified of the Data Breach via a Breach Notice letter which indicated Plaintiff Tompkins' Personal Information had been exposed in the Data Breach.

15. Plaintiff Kenneth Brennan is a citizen of Arizona residing in Tucson, Arizona. Plaintiff Brennan is a Data Breach victim and a patient of Radiology Ltd., a US Radiology Partner. Plaintiff Brennan was notified of the Data Breach via a Breach Notice letter which indicated Plaintiff Brennan's Personal Information had been exposed in the Data Breach.

16. Plaintiff Chandra Brown is a citizen of Alabama. Plaintiff Brown is a Data Breach victim and a patient of American Health Imaging, a US Radiology Partner. Plaintiff Brown was notified of the Data Breach via a Breach Notice Letter which indicated Plaintiff Brown's Personal Information had been exposed in the Data Breach.

17. Defendant US Radiology partners with physician-owned radiology practices and diagnostic imaging centers with its principal place of business located at 4200 Six Forks Road, Suite 100, Raleigh, NC 27609.

18. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

19. All of Plaintiffs' claims stated herein are asserted against Defendant and its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

20. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

21. This Court has personal jurisdiction over the Defendant named in this action because Defendant is headquartered in this District and Defendant conducts substantial business in North Carolina and this District through its headquarters, offices, parents, and affiliates.

22. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

23. US Radiology is a medical company that partners with top private practice radiology groups, outpatient imaging operators, and leading health systems. Sharing best practices, US Radiology claims that by investing in a partnership with US Radiology, radiology groups across the country can elevate patient care.

24. US Radiology advertises that its program ensures that physician partners are "setting the standard in our field: providing top-level, evidence-based care and generating the

highest quality outcomes."[5]

25. US Radiology further advertises that it can help its partners drive productivity and improve processes and patient outcomes through innovative technology and equipment that may not be accessible or affordable for an independent practice or imaging center. US Radiology claims that its investments in areas including "next-generation stack systems, revenue cycle management and database analytics" will help practices streamline operational and financial processes.[6]

26. US Radiology's "Partners" include: Charlotte Radiology, Diversified Radiology, Touchstone Medical Imaging, American Health Imaging, Radiology Ltd., Upstate Carolina Radiology, Windsong Radiology, Gateway Diagnostic Imaging, South Jersey Radiology Associates, and Larchmont Imaging Associates.[7]

27. Upon information and belief, through its Partners, Defendant receives, collects and stores some of Plaintiffs' and Class Members' most sensitive and confidential information, including their Social Security numbers, as a condition of rendering medical services.

28. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their Personal Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their Personal Information.

29. Defendant, as a healthcare company retaining Personal Information of patients, had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Personal Information from involuntary disclosure to third parties.

The Data Breach

[5] *See* https://www.usradiology.com/why-us-radiology (last accessed Oct. 8, 2022).
[6] *See id.*
[7] *See* https://www.usradiology.com/partners (last accessed Oct. 10, 2022).

30. Although US Radiology has yet to formally acknowledge to Plaintiffs and Class Members that it was the source of a Data Breach affecting hundreds of thousands of individuals, at least eight of its ten Partners have announced identical cybersecurity incidents, pointing towards US Radiology as the entity responsible for releasing Plaintiffs' and Class Members' Personal Information.

31. In February 2022, US Radiology made a report to HHS regarding a cybersecurity incident that compromised Personal Information of 87,552 patients.[8] US Radiology did not provide any additional context as to the details of this cybersecurity incident. Upon information and belief, this is the only acknowledgement of the Data Breach US Radiology has made to date.

32. In the months following US Radiology's report to HHS, Texas's Attorney General's Office received reports from both Gateway Diagnostics and American Health Imaging, two of US Radiology's Partners, notifying the Office of a Data Breach impacting 240,673 Texas Gateway Diagnostics patients and 21,003 Texas American Health Imaging patients. Gateway Diagnostic Imaging and Radiology Ltd. also submitted breach notices to the Montana Attorney General's office.

33. As of the filing of this complaint, Touchstone Medical Imaging, Charlotte Radiology, Radiology Ltd., Gateway Diagnostics, American Health Imaging, Windsong Radiology[9], Diversified Radiology, and Upstate Carolina Radiology, have all issued public notices of the Data Breach ("Breach Notices"), which Plaintiffs believe are all connected.[10] The Breach

[8] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Sept. 26, 2022).
[9] Upon information and belief, Windsong Radiology acquired Buffalo MRI in August 2021. Buffalo MRI has publicized notice of the Data Breach.
[10] *See* **Exhibit 1** – Touchstone Medical Breach Notice, **Exhibit 2** – Charlotte Radiology Breach Notice, **Exhibit 3** – Radiology Ltd. Breach Notice, **Exhibit 4** – Gateway Diagnostics Breach Notice, **Exhibit 5** – American Health Imaging Breach Notice, **Exhibit 6** – Buffalo MRI Breach Notice, **Exhibit 7** – Diversified Radiology Breach Notice, **Exhibit 8** – Upstate Carolina Breach Notice.

Notices are near identical in both substance and form:

> **Notice of IT Security Incident Affecting Certain Patients**
>
> In late 2021, Touchstone Medical Imaging experienced an incident that involved certain patients' information. We have completed our investigation and there is no evidence that this incident resulted in fraud or misuse of the information involved. We expect to complete the notification process for all identified individuals by the end of September.
>
> On December 24, 2021, we identified a security incident that impacted systems that contained our patient information. We immediately initiated our incident response process, notified law enforcement, and began an investigation with the assistance of a forensic firm. Within days, we were able to contain the incident and resume serving patients. The investigation subsequently determined that between December 17 and December 24, 2021, an unauthorized party gained access to our network.
>
> Some patients' information may have been accessed, including patient names and one or more of the following: address, date of birth, health insurance information, medical record number, patient account number, physician name, date(s) of service, diagnosis, and/or treatment information related to radiology services. For a limited number of patients, Social Security numbers may have been included. We are offering complimentary credit monitoring to those individuals.
>
> We recommend that patients review the statements they receive from their health insurer. If you see charges for services you did not receive, please call the insurer immediately.
>
> We have also set up a dedicated call center to answer questions about this incident. Patients with questions may call the call center at 1-855-604-1852, Monday through Friday between 8 AM – 8 PM Central Time.
>
> We continue to implement enhancements to information security, systems, and monitoring capabilities and are committed to maintaining the confidentiality and security of patients' information.

See Exhibit 1.

34. Not only do all eight Breach Notices reference a Data Breach that occurred between December 17 and December 24, 2021, where an unauthorized party gained access to Personal Information, all eight Breach Notices also provide the same phone number for a dedicated call center to provide answers to questions regarding the Data Breach and recommend the same course of action for victims to protect themselves.

35. Upon information and belief, the true source of the Data Breach was US Radiology, the common link between the Partners. US Radiology has refused to be transparent with Plaintiffs and Class Members regarding the circumstances under which their Personal Information was exposed to unauthorized third parties, which is required under both state and federal law.

36. US Radiology did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing their Personal Information to be exposed.

37. Given that Defendant was storing the Personal Information of hundreds of thousands of individuals, Defendant could have and should have implemented industry-standard measures to prevent and detect cybersecurity incidents.

38. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[12]

39. The ramifications of Defendant's failure to keep secure the Personal Information of Plaintiffs and Class Members are long lasting and severe. Once stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

40. The Personal Information of individuals remains of high value to criminals, as

[11] 17 C.F.R. § 248.201 (2013).
[12] *Id.*

evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[13] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

41. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[16]

42. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual,

---

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 2, 2022).

[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 2, 2022).

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 2, 2022).

[16] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 2, 2022).

ongoing fraud activity to obtain a new number.

43. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

44. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, Social Security number, and potentially date of birth.

45. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[18]

46. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

47. The Personal Information of Plaintiffs and Class Members was taken by hackers to engage in identity theft and/or to sell it to other criminals who will purchase the Personal Information for that purpose. The fraudulent activity resulting from the Data Breach may not come

[17] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Aug. 1, 2022).

[18] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 2, 2022).

to light for years.

48. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

49. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Personal Information of Plaintiffs and Class Members, including Social Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if the Personal Information was compromised, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members a result.

50. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more industry-standard measures to prevent cybersecurity incidents, resulting in the Data Breach and the exposure of the PII of hundreds of thousands of individuals, including Plaintiffs and Class Members.

The Healthcare Sector is Particularly Vulnerable to Ransomware Attacks

51. Defendant was on notice that companies in the healthcare industry are targets for data breaches.

52. Defendant was on further notice regarding the increased risks of inadequate

[19] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/products/gao-07-737 (last visited Aug. 1, 2022).

cybersecurity. In February 2022, the cybersecurity arm of HHS issued a warning to hospitals and healthcare systems about a dramatic rise in cyberattacks, urging facilities to strengthen up their cyber defenses.[20] Indeed, HHS's cybersecurity arm recently issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.[21]

53. In the context of data breaches, healthcare is "by far the most affected industry sector."[22] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed Personal Information.[23] A Tenable study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in *nearly 93% of the breaches*."[24]

54. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or

[20] Rebecca Pifer, *Tenet says 'cybersecurity incident' disrupted hospital operations*, HEALTHCAREDIVE (Apr. 26, 2022), https://www.healthcaredive.com/news/tenet-says-cybersecurity-incident-disrupted-hospital-operations/622692/.
[21] *Id.* (HHS warned healthcare providers about the increased potential for attacks by a ransomware group called Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said reports have linked Hive to attacks on 355 companies within 100 days of its launch last June — nearly three a day.").
[22] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed Oct. 11, 2022).
[23] *Id.*
[24] *Id.*

Personally Identifiable Information (PII)."[25]

55. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[26]

56. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[27] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[28] That trend continues through 2022.

57. When compromised, healthcare-related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore

---

[25] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at*: https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Aug. 1, 2022).

[26] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last accessed Oct. 7, 2022).

[27] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.idtheftcenter.org/surveys-studys (last accessed Oct. 7, 2022).

[28] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/2017-data-breaches/ (last accessed Oct. 7, 2022).

coverage.[29] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[30]

Plaintiffs and Class Members Have Suffered Harm Resulting From the Data Breach

58. This case involves a cybersecurity incident that resulted in the unauthorized access, disclosure, and/or acquisition of the Personal Information of Plaintiffs and Class Members to unknown third-parties. The Personal Information of Plaintiffs and Class Members is likely now in the hands of criminals.

59. Once information is placed onto the internet, it is virtually impossible to remove. Plaintiffs and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiffs and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Defendant's failures.

60. By obtaining, collecting, using, and deriving a benefit from the Personal Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access, intrusion, and/or acquisition.

61. Moreover, Defendant now puts the burden squarely on Plaintiffs and Class Members to enroll in the inadequate monitoring services offered to some of them, among other steps Plaintiffs and Class Members must take to protect themselves. Time is a compensable and

[29] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Oct. 7, 2022).
[30] *Id.*

valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[31]

62. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[32] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[33] Usually, this time can be spent at the option and choice of the individual, however, having been notified of the Data Breach, Plaintiffs and Class Members now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

63. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

64. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Personal Information is used;

---

[31] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, *available at* https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed Oct. 2, 2022); *see also* U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data, available at* https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last accessed Oct. 2, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.).

[32] *See* https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (last visited Oct. 2, 2022).

[33] *Id.*

b. The diminution in value of their Personal Information;

c. The compromise and continuing publication of their Personal Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Personal Information; and

h. The continued risk to their Personal Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII and PHI in its possession.

65. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their Personal Information.

66. To date, only a "limited number" of Class Members have been offered complimentary credit monitoring services as a result of the Data Breach. The offered service is wholly inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the Personal Information at issue here.

67. Further, there is a market for Plaintiffs' and Class Members' Personal Information. Sensitive healthcare data can sell for as much as $363 per record according to the Infosec Institute.

68. Medical information, like the information exposed in the Data Breach, is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Personal Information on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

69. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[34]

70. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Personal Information of Plaintiffs and Class Members.

Defendant's Conduct Violates the Rules and Regulations of HIPAA and HITECH

71. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that HHS

[34] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), *available at* https://khn.org/news/rise-of-indentity-theft/ (last visited Oct. 2, 2022).

create rules to streamline the standards for handling Personal Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

72. Defendant is a covered entity pursuant to HIPAA. *See* 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

73. Defendant is a covered entity pursuant to the Health Information Technology Act ("HITECH").[35] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

74. Plaintiffs' and Class Members' Personal Information is "protected health information" as defined by 45 CFR § 160.103.

75. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

76. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

77. Plaintiffs' and Class Members' Personal Information is "unsecured protected health information" as defined by 45 CFR § 164.402.

78. Plaintiffs' and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

79. Plaintiffs' and Class Members' unsecured protected health information acquired,

[35] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

80. Plaintiffs' and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

81. Plaintiffs' and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

82. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

83. The Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of Personal Information when it was no longer necessary and/or had honored its obligations to its patients.

84. It can be inferred from Defendant's Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiffs and Class Members' Personal Information.

85. Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health

information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502,et seq.; and

k. Retaining information past a recognized purpose and not deleting it.

86. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and **in no case later than 60 days following discovery of the breach**." Upon information and belief, US Radiology has **still not notified** Plaintiffs and Class Members of the Data Breach that occurred in December 2021. Indeed, the Breach Notices from Defendant's Partners indicate that the notification process was expected to be completed by the end of September 2022.[36]

87. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiffs and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the protected health information and other Personal Information of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Plaintiffs' and Class Members' protected health information and other Personal Information remains at risk of subsequent Data Breaches.

Plaintiffs' Experiences

88. Plaintiff Tompkins is a former patient of Gateway Diagnostics, a Partner of US Radiology.

89. As a condition of receiving medical services from Gateway Diagnostics, Plaintiff Tompkins provided Gateway Diagnostics with her name, address, telephone number, date of birth, Social Security number, and other Personal Information. Gateway Diagnostics also maintained records of Plaintiff's medical history and treatment information related to radiology services.

[36] *See* Exhibit 1.

90. Upon information and belief, Plaintiff Tompkins's Personal Information was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

91. Plaintiff Tompkins received a Notice of Data Breach from Gateway Diagnostics stating that her Personal Information was compromised in the Data Breach.

92. As a result of the Data Breach, Plaintiff Tompkins has spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through her unsolicited emails and text messages, time spent verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

93. Further, Plaintiff Tompkins has experienced an uptick in spam telephone calls, emails and text messages since the Data Breach.

94. Plaintiff Tompkins is very careful about sharing her Personal Information. She has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source.

95. Plaintiff Tompkins stores any documents containing her Personal Information in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for his online accounts.

96. Plaintiff Brennan is a patient of Radiology Ltd., a US Radiology Partner. Over the last several years, Plaintiff Brennan has made several visits to Radiology Ltd to receive medical services.

97. As a condition of receiving medical services from Radiology Ltd., Plaintiff Brennan provided Radiology Ltd. with his name, address, telephone number, date of birth, Social Security

number, and other Personal Information. Radiology Ltd. also maintained records of Plaintiff's medical history and treatment information related to radiology services.

98. Upon information and belief, Plaintiff Brennan's Personal Information was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

99. Plaintiff Brennan received a Notice of Data Breach from Radiology Ltd. on or around September 2, 2022, stating that his Personal Information was compromised in the Data Breach.

100. As a result of the Data Breach, Plaintiff Brennan has spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through his unsolicited emails and text messages, time spent verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, reviewing the credit monitoring service offered by Defendant, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

101. Further, Plaintiff Brennan has experienced actual fraud as a result of the Data Breach. Following the Data Breach, Plaintiff Brennan discovered various fraudulent charges on his Bank of America credit card. Approximately six charges appeared on his credit card and were set up as monthly, recurring charges for a variety of items such as online gaming.

102. Plaintiff Brennan contacted the Bank of America fraud department, who informed him that this was "fishing" activity that would escalate to higher charges if Brennan did not act quickly enough to end the fraudulent activity. Bank of America cancelled the fraudulent charges and cancelled Plaintiff Brennan's credit card and issued him a new credit card and debit card.

103. As a result of the Data Breach and out of concern for the security of his Personal Information, Plaintiff Brennan purchased Experian Credit Monitoring Protection services.

104. Plaintiff Brennan is very careful about sharing his Personal Information. He has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source.

105. Plaintiff Brennan stores any documents containing his Personal Information in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

106. Plaintiff Brown is a former patient of American Health Imaging, a US Radiology Partner. During the years 2017 to 2021, Plaintiff Brown made several visits to American Health Imaging to receive medical services.

107. As a condition of receiving medical services from American Health Imaging, Plaintiff Brown provided American Health Imaging with her name, address, telephone number, date of birth, Social Security number, and other Personal Information. American Health Imaging also maintained records of Plaintiff's medical history and treatment information related to radiology services.

108. Upon information and belief, Plaintiff Brown's Personal Information was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

109. Plaintiff Brown received a Notice of Data Breach from American Health Imaging on or around August 15, 2022, stating that her Personal Information was compromised in the Data Breach.

110. Plaintiff Brown has also spent time and energy sorting through her unsolicited emails and text messages, time spent verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, reviewing the credit monitoring service offered

by Defendant, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

111. Plaintiff Brown has experienced actual fraud as a result of the Data Breach. Shortly after the Data Breach, Plaintiff Brown received an invoice from American Health Imaging for a service from 5 years ago. This invoice was for an injury which occurred while at her place of employment and the recent reveal of this unpaid invoice has caused great hardship on her employer and her status with her employer. Plaintiff Brown has spent approximately 30 hours trying to correct this issue with American Health Imaging.

112. Plaintiff Brown is very careful about sharing her Personal Information. She has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source.

113. Plaintiff Brown enrolled in a credit monitoring service and notified a major credit reporting service to issue a freeze on her credit causing additional hardship, emotional stress and lost time that she will not recover.

114. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their Personal Information—a form of intangible property that Plaintiffs entrusted to Defendant for the purpose of receiving medical care, which was compromised in and as a result of the Data Breach.

115. Plaintiffs suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have anxiety and increased concerns for the loss of their privacy.

116. Plaintiffs are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from their Personal Information, especially their Social Security numbers, in combination with their names, being placed in the hands of unauthorized third parties and

criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiffs' Personal Information.

117. Plaintiffs have a continuing interest in ensuring that their Personal Information, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

118. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

119. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose Personal Information was compromised during the December 2021 Data Breach affecting US Radiology and/or its Partners. (the "Nationwide Class").

120. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

121. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

122. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable

class. A well-defined community of interest exists to warrant class wide relief because Plaintiffs and all members of the Nationwide Class were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

123. The Nationwide Class is so numerous that individual joinder of its members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, Plaintiffs are informed and believes that there are at least hundreds of thousands of Class Members.

124. Common questions of law and fact exist as to members of the Nationwide Class and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

a. Whether and to what extent Defendant had a duty to protect the Personal Information of Plaintiffs and Class Members;

b. Whether Defendant had a duty not to disclose the Personal Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the Personal Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Personal Information of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Personal Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Personal Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures

and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Personal Information of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

125. Plaintiffs are members of the Class they seek to represent and their claims and injuries are typical of the claims and injuries of the other Class Members.

126. Plaintiffs will adequately and fairly protect the interests of other Class Members. Plaintiffs have no interests adverse to the interests of absent Class Members. Plaintiffs are represented by legal counsel with substantial experience in class action litigation. The interests of Class Members will be fairly and adequately protected by Plaintiffs and their counsel.

127. Defendant has acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

128. A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action

treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them. Further, class litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiffs are unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

129. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 117.

130. Defendant owed to Plaintiffs and Class Members a duty to exercise reasonable care in handling and using the Personal Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from breach, theft, and unauthorized use.

131. Plaintiffs and the Nationwide Class provided certain Personal Information as a condition of receiving medical services and care based upon the premise and with the understanding that their Personal Information would be safeguarded, would be used for business purposes only, and/or not disclosed to unauthorized third parties.

132. Defendant has full knowledge of the sensitivity of the Personal Information and the

types of harm that Plaintiffs and the Nationwide Class could and would suffer if the Personal Information were wrongfully disclosed.

133. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Personal Information of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

134. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Personal Information of Plaintiffs and the Nationwide Class in Defendant's possession was adequately secured and protected.

135. Defendant owed a duty to Plaintiffs and the Nationwide Class to implement intrusion detection processes that would detect a data breach or unauthorized access to its systems in a timely manner.

136. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Personal Information it was no longer required to retain pursuant to regulations, including that of former patients.

137. Defendant also had a duty to employ proper procedures to detect and prevent the improper access, misuse, acquisition, and/or dissemination of the Personal Information of Plaintiffs and the Nationwide Class.

138. Defendant owed a duty to disclose the material fact that Defendant's data security practices were inadequate to safeguard the personal and medical information of Plaintiffs and the Nationwide Class.

139. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

140. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Personal Information of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that Personal Information, and the necessity for encrypting Personal Information stored on Defendant's systems.

141. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the Personal Information of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendant.

142. Plaintiffs and the Nationwide Class had no ability to protect their Personal Information that was in, and likely remains in, Defendant's possession.

143. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

144. Defendant had and continues to have a duty to adequately disclose that the Personal Information of Plaintiffs and the Nationwide Class within Defendant's possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Personal Information

by third parties.

145. Defendant has admitted that the Personal Information of Plaintiffs and the Nationwide Class was wrongfully accessed, acquired, and/or released to unauthorized third persons as a result of the Data Breach.

146. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Personal Information of Plaintiffs and the Nationwide Class during the time the Personal Information was within Defendant's possession or control.

147. Defendant improperly and inadequately safeguarded the Personal Information of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

148. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Personal Information of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

149. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect unauthorized access or intrusions and prevent dissemination of their Personal Information. Additionally, Defendant failed to disclose to Plaintiffs and the Nationwide Class that Defendant's security practices were inadequate to safeguard the Personal Information of Plaintiffs and the Nationwide Class.

150. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Personal Information it was no longer required to retain pursuant to regulations,

including PII of former patients and employees.

151. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

152. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Personal Information.

153. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and Class Members' Personal Information.

154. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Nationwide Class.

155. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

156. Plaintiffs and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

157. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and

deceptive practices, caused the same harm as that suffered by Plaintiffs and the Nationwide Class.

158. Defendant's violations of HIPAA and HITECH also independently constitute negligence *per se*.

159. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

160. Plaintiffs and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

161. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

162. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the Personal Information of Plaintiffs and the Nationwide Class would not have been compromised.

163. There is a close causal connection between Defendant's failure to implement security measures to protect the Personal Information of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The Personal Information of Plaintiffs and the Nationwide Class was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Personal Information by adopting, implementing, and maintaining appropriate security measures.

164. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer injury.

165. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their Personal Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

166. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages. Plaintiffs and Class members are also entitled to the injunctive relief sought herein.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

167. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 117.

168. Plaintiffs and the Nationwide Class provided and entrusted their Personal Information as a condition of obtaining medical care from Defendant's Partners.

169. Plaintiffs and the Nationwide Class paid money to Defendant's Partners and, upon information and belief, to Defendant, in exchange for goods and services, as well as the promises to protect their protected health information and other Personal Information from unauthorized disclosure.

170. Plaintiffs and the Nationwide Class entered into implied contracts with Defendant and Defendant's Partners by which Defendant agreed to safeguard and protect such information,

to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Nationwide Class if their data had been breached and compromised or stolen.

171. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete Personal Information and to pay Defendant and Defendant's Partners in exchange for Defendant's agreement to, *inter alia*, protect their Personal Information.

172. Plaintiffs and the Nationwide Class Members would not have entrusted their Personal Information to Defendant or Defendant's Partners in the absence of Defendant's implied promise to adequately safeguard this confidential personal and medical information.

173. Plaintiffs and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

174. Defendant breached the implied contracts it made with Plaintiffs and the Nationwide Class by making their Personal Information accessible and by failing to make reasonable efforts to use the latest security technologies designed to help ensure that the Personal Information was secure, failing to encrypt Plaintiffs and Class Members' sensitive Personal Information, failing to safeguard and protect their Personal Information, and by failing to provide timely and accurate notice to them that Personal Information was compromised as a result of the Data Breach.

175. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to comply with its promise to abide by HIPAA and HITECH.

176. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

177. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

178. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

179. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

180. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

181. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

182. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

183. Defendant further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that

is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

184. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

185. Defendant further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Personal Information.

186. Defendant's failures to meet these promises constitute breaches of the implied contracts.

187. Because Defendant allowed unauthorized access to Plaintiffs' and Class Members' Personal Information and failed to safeguard the Personal Information, Defendant breached its contracts with Plaintiffs and Class Members.

188. Defendant breached its contracts by not meeting the minimum level of protection of Plaintiffs' and Class Members' protected health information and other Personal Information, because Defendant did not prevent against the breach of hundreds of thousands of individuals' Personal Information.

189. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendant providing goods and services to Plaintiffs and Class Members that were of a diminished value.

190. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Nationwide Class are now subject to the present and continuing risk of fraud, and are suffering (and will continue to suffer) the ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual

identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the diminished value of services provided by Defendant; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

191. As a result of Defendant's breach of implied contract, Plaintiffs and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class)

192. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 117.

193. Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and the Nationwide Class's Personal Information that Defendant was using and storing.

194. As alleged herein and above, Defendant's relationship with Plaintiffs and the Nationwide Class was governed by terms and expectations that Plaintiffs' and the Nationwide Class's Personal Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

195. Plaintiffs and the Nationwide Class provided their Personal Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Personal Information to be disseminated to any unauthorized third parties.

196. Plaintiffs and the Nationwide Class also provided their Personal Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Personal Information from unauthorized disclosure.

197. Defendant voluntarily received in confidence the Personal Information of Plaintiffs and the Nationwide Class with the understanding that Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

198. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the Personal Information of Plaintiffs and the Nationwide Class was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs and the Nationwide Class's confidence, and without their express permission.

199. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and the Nationwide Class have suffered damages.

200. But for Defendant's disclosure of Plaintiffs' and the Nationwide Class's Personal Information in violation of the parties' understanding of confidence, their Personal Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiffs' and the Nationwide Class's PII as well as the resulting damages.

201. The injury and harm Plaintiffs and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs and the Nationwide Class's Personal Information. Defendant knew or should have known its methods of accepting and securing Plaintiffs and the Nationwide Class's Personal Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs and the Nationwide Class's Personal Information.

202. As a direct and proximate result of Defendant's breach of its confidence with Plaintiffs and the Nationwide Class, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

203. As a result of Defendant's breaches of confidence, Plaintiffs and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

204. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 117.

205. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of their Personal Information, as this was used to facilitate payment for Defendant's services.

206. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs and Class Members.

207. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount to be determined at trial.

208. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself that were mandated by federal, state, and local laws and industry standards.

209. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct

complained of herein pertaining to the misuse and/or disclosure of the Personal Information of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Personal Information of Plaintiffs and Class Members;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, nominal, and statutory damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, by counsel, hereby demands that this matter be tried before a jury.

Date: October 25, 2022

Respectfully Submitted,

/s/ Jean S. Martin
JEAN S. MARTIN
(North Carolina State Bar No. 25703)
FRANCESCA KESTER*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jeanmartin@ForThePeople.com
fkester@ForThePeople.com

ELAINE A. RYAN*
COLLEEN M. AUER*
AUER RYAN, P.C.
20987 N. John Wayne Parkway, #B104-374
Maricopa, AZ 85139 520-705-7332
eryan@auer-ryan.com
cauer@auer-ryan.com

Joseph P. Tunstall III
(North Carolina State Bar No. 29477)
O'MALLEY TUNSTALL PLLC
PO BOX 1158
Tarboro, NC 27886
(252) 823-2266
jptunstall@omalleytunstall.com

Attorneys for Plaintiffs and the Putative Class

**Pro Hac Vice Application Forthcoming*